

ABSTRACT

An authentication method and schemes using a block cipher to protect data integrity (authenticity) during communication over insecure channels and during data storage on insecure media. The authentication method and schemes of this invention allow, in a further aspect, message and data signing and verification in parallel or pipelined manners, in addition to sequential operation, without requiring twice as many block enciphering operations as the number of input plaintext blocks. The present invention allows, in a yet further aspect, software and hardware implementations used in high-performance systems and networks where multiple processing units are available for block enciphering operations. In a yet further aspect, the authentication method and schemes of this invention allow incremental updates and out-of-order processing of authentication tags. In a yet further aspect, the authentication method and schemes of this invention are suitable for real-time applications where message length remains unknown until the entire message is received, and commencing message authentication cannot be deferred until the end of the message.